(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 385 303 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.01.2004 Bulletin 2004/05

(51) Int Cl.[7]: **H04L 12/58**, H04L 29/06

(21) Application number: **03254532.9**

(22) Date of filing: **17.07.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **22.07.2002 US 397922 P**
25.09.2002 US 255658

(71) Applicant: **SYMANTEC CORPORATION**
Cupertino, CA 95014 (US)

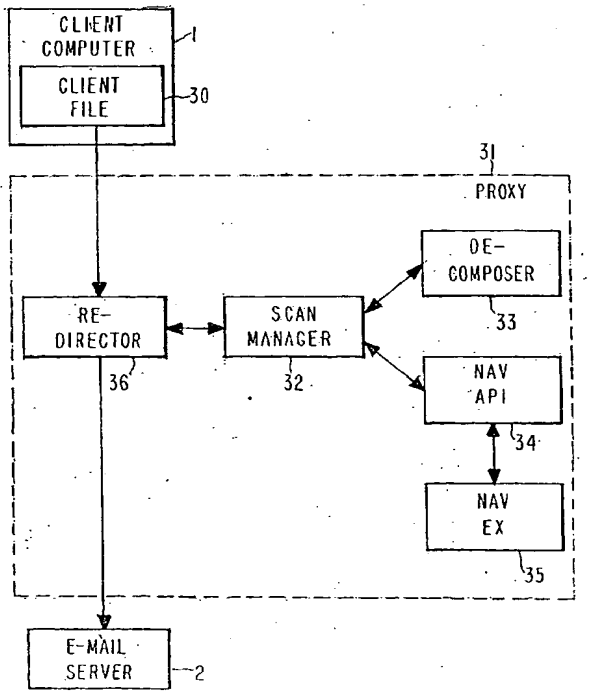
(72) Inventor: **Szor, Peter**
Northridge, CA 91326 (US)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
16 High Holborn
London WC1V 6BX (GB)

(54) Method and device for preventing malicious computer code from propagating

(57) Computer-implemented methods, systems, and computer-readable media for detecting the presence of malicious computer code in an e-mail sent from a client computer (1) to an e-mail server (2). An embodiment of the inventive method comprises the steps of: interposing (41) an e-mail proxy server (31) between the client computer (1) and the e-mail server (2); allowing (42) the proxy server (31) to intercept e-mails sent from the client computer (1) to the e-mail server (2); enabling (43) the proxy server (31) to determine when a file (30) is attempting to send itself (30) as part of an e-mail; and declaring (44) a suspicion of malicious computer code when the proxy server (31) determines that a file (30) is attempting to send itself (30) as part of an e-mail.

FIG. 3



EP 1 385 303 A2

Description

[0001] This invention pertains to the field of preventing malicious attacks to computers, and, in particular, preventing e-mail propagation of malicious computer code.

[0002] As used herein, "malicious computer code" is any code that enters a computer without an authorized user's knowledge and/or without an authorized user's consent. Malicious computer code that propagates from one computer to another over a network, e.g., via e-mail, is often referred to as a "worm". Most worms that spread from one computer to another are spread via e-mail over the Internet. The most common way to send e-mail over the Internet is using the SMTP (Simple Mail Transfer Protocol). SMTP is part of TCP/IP (Transfer Control Protocol/Internet Protocol). SMTP was originally designed to send only that e-mail that consists solely of text and that is encoded using the ASCII character set, which is limited. It soon became apparent that computer users wished to send other than straight ASCII characters as e-mail, and so encoding schemes such as UUencode and MIME were developed. These encoding schemes are capable of encoding any type of file, including a binary graphics file, into ASCII so that it can be sent as an e-mail attachment.

[0003] Figure 1 illustrates a common system by which a client computer 1 can send e-mail to a recipient computer 5 over an open network 4 such as the Internet. In Figure 1, it is assumed that there are a plurality N of client computers 1 located within an enterprise 3. Enterprise 3 may be a company, a university, a government agency, etc. Computers 1 are coupled to each other and to an e-mail server computer 2 over a Local Area Network (LAN) 6. E-mail server 2 collects and formats e-mails sent from computers 1 and sends them to the designated recipients 5 using the SMTP protocol. It is assumed that there are a plurality J of recipient computers.

[0004] Figure 2 illustrates a similar network in which client computers 1 are not associated with the same enterprise 3, but rather may be more geographically dispersed and are subscribers to an Internet Service Provider (ISP). In this case, computers 1 communicate with the ISP's e-mail server 2 via the Public Switched Telephone Network (PSTN) 6. In other respects, the functioning of the networks illustrated in Figures 1 and 2 are the same.

Disclosure of Invention

[0005] Computer-implemented methods, systems, and computer-readable media for detecting the presence of malicious computer code in an e-mail sent from a client computer (1) to an e-mail server (2). An embodiment of the inventive method comprises the steps of: interposing (41) an e-mail proxy server (31) between the client computer (1) and the e-mail server (2); allowing (42) the proxy server (31) to intercept e-mails sent from the client computer (1) to the e-mail server (2); enabling (43) the proxy server (31) to determine when a file (30) is attempting to send itself (30) as part of an e-mail; and declaring (44) a suspicion of malicious computer code when the proxy server (31) determines that a file (30) is attempting to send itself (30) as part of an e-mail.

Brief Description of the Drawings

[0006] These and other more detailed and specific objects and features of the present invention are more fully disclosed in the following specification, reference being had to the accompanying drawings, in which:

Figure 1 is a system level diagram of a conventional network for sending e-mail from within an enterprise 3.

Figure 2 is a system level diagram of a conventional network for sending e-mail via an Internet Service Provider (ISP) computer 2.

Figure 3 is a block diagram illustrating an embodiment of the present invention.

Figure 4 is a flow diagram illustrating an embodiment of the present invention.

Detailed Description of the Preferred Embodiments

[0007] Nefarious persons sending malicious computer code via e-mails have resorted to many tricks to spread their malicious messages. A typical e-mail may look something like this:

```
IP x.y.z.1:25 (SMTP)
HELLO      someone
RCPT to: edGXYZ.com
FROM: XYZGx17as.com
SUBJECT: HELLO
DATA
MIME-encoded attachments
```

[0008] One of the tricks employed by authors of malicious code is to falsify the "FROM" field so that the recipient of the e-mail will be lulled into thinking that the e-mail was sent from a known, reputable source.

[0009] Sometimes the malicious code will be encrypted, making it difficult for a conventional anti-virus scanner to analyze it.

[0010] Modern worms such as Klez self-activate simply by the user clicking open the e-mail message itself: the user doesn't even have to click on the e-mail attachment containing the worm. Klez has operated through the popular e-mail software known as Microsoft Outlook. Klez contains its own SMTP client embedded in the worm; it does not rely on Outlook.

[0011] The present invention thwarts the propagation

of malicious computer code being sent in an email from a client computer 1 to an e-mail server 2, by means of interposing (step 41 of Fig. 4) an e-mail proxy server 31 (hereinafter referred to as "proxy") between the client computer 1 and the e-mail server 2. The client computer 1 thinks that the proxy 31 is the real e-mail server 2. The proxy 31 may be associated with the client computer 1, e.g., it may reside within computer 1.

[0012] Figure 3 illustrates the basic architecture of proxy 31. Redirector 36 intercepts e-mail messages, and tricks client file 30 into thinking that redirector 36 is e-mail server 2. Scan manager 32 is coupled to re-director 36, and contains intelligence for examining the contents of e-mails. Decomposer 33 is coupled to scan manager 32; and unpacks (e.g., unzips) objects and sends the decomposed objects back to scan manager 32 one by one. Decomposer 33 is invoked when the e-mail being analyzed by scan manager 32 contains many objects, e.g., an e-mail body and several e-mail attachments that are zipped or otherwise combined. In that case, decomposer 33 unzips the objects and presents them to scan manager 32 one by one for further analysis. API 34 such as Norton Antivirus Application Programming Interface (NAVAPI) 34 is coupled to scan manager 32, and presents scan manager 32 with ready access to conventional antivirus software. Extensions 35 such as Norton Antivirus Extensions (NAVEX) 35 are coupled to NAVAPI 34 and contain all of the scanning engines, virus signatures, and virus names used in conventional antivirus scanning. Modules 31-36 may be implemented in hardware, software, and/or firmware, or any combination thereof.

[0013] In the embodiment where e-mail server 2 adheres to the SMTP protocol, proxy 31 adheres to the SMTP protocol as well.-Generally speaking, proxy 31 adheres to the same protocol adhered to by e-mail server 2.

[0014] At step 42 of Fig. 4, proxy 31 is enabled to intercept e-mail sent from the client computer 1 to the e-mail server 2. The enabling may be accomplished by the user of computer 1 clicking on a "e-mail scanning" feature on antivirus software (such as Norton Antivirus manufactured by Symantec Corporation of Cupertino, California) that has been installed on the user's computer 1. Such an enabling may, for example, serve to activate proxy 31 every time a client file 30 within client computer 1 attempts to access the computer's port 25, which is the conventional port used in personal computers for sending e-mail over the Internet.

[0015] At step 43, scan manager 32 determines whether file 30 is attempting to send itself, either as part of the e-mail body or as an e-mail attachment. The determination that is made in step 43 can vary based upon the type of file 30. The name of the file 30 is ascertained by redirector 36 and given to scan manager 32. In the WIN32 API of Microsoft Corporation, scan manager 32 determines whether file 30 is a file in the PE (portable executable) format. The PE header identifies file 30 as a PE file. Section headers determine the type of the section, e.g., code sections, data sections, resource sections, etc. For a PE file in the WIN 32 API, scan manager 32 examines the entire code section or code sections. Scan manager 32 performs a compare between two versions of file 30: the version that has been intercepted and that now resides within proxy 31 versus the version that resides in client computer 1. In one embodiment, scan manager 32 declares a suspicion of malicious code in step 44 when the two versions are nearly identical. If the two versions are not nearly identical, scan manager 32 declares in step 45 that no malicious code is present in file 30. "Nearly identical" is defined throughout this patent application to mean that no more than one byte out of a preselected threshold number of bytes varies between the two versions. In one embodiment, the preselected threshold number of bytes is 512. Other preselected threshold numbers can be selected based on the application. The reason for not insisting upon perfect matching between the two versions of the file is that the malicious code occasionally modifies a byte of the file.

[0016] Once a suspicion of malicious code is declared in step 44, one or more optional steps 46, 47, and 48 can be invoked. Steps 46 and 48 serve to reduce the number of unwanted false positives (declaring a file 30 to be contaminated when it isn't).

[0017] In optional step 46, the user of computer 1 is given a set of choices when a suspicion of malicious code has been declared in step 44. These choices may be presented to the user via a dialog box which pops up on the user's monitor. Such a dialog box may look like the following:

Malicious Worm Alert
Filename: readme.exe

[0018] Norton AntiVirus has detected a malicious worm on your computer that is trying to e-mail itself to other computers. If . this Malicious Worm Alert appeared when you were not sending an e-mail message, the worm is trying to spread itself by e-mail, and you should select the "Quarantine this worm (Recommended)" option from the following drop down list. You can get more information about the worm from the Symantec Security Response virus encyclopedia.

[0019] Select one of the following actions:

- Stop this worm from e-mailing itself. This stops the worm from e-mailing itself at this time, but does not quarantine the worm. This action leaves the worm on your computer, where it can possibly be activated again. Select this option only if you are sure you want to leave the worm on your computer.
- Quarantine this worm (Recommended). This permanently stops the worm by putting it in the Norton

AntiVirus Quarantine. While in Quarantine, the worm will not be able to spread itself. This is the safest action.

- Allow this application to send e-mail attachments. This sends the e-mail containing a potential worm. Such a worm could infect the recipient's computer. Select this option only if you are sure the e-mail is not infected with a worm.
- Always allow this application to send e-mail attachments. In the future, Norton AntiVirus will not check this file for worms. This is the riskiest action, because such a worm could e-mail itself from your computer without your knowledge.

[0020] Note that the file name of the suspicious file 30 is given to the user, along with four choices. If the second choice is selected (quarantining the worm), file 30 is encrypted and sent to the headquarters of the antivirus company (in this case, Symantec) for analysis.

[0021] It is expected that the user would rarely select choices three or four (allowing the application to send e-mail attachments). Such a choice might be selected when the user is attempting to e-mail the entire e-mail software program to a recipient.5.

[0022] In optional step 47, an alert is sent to every client computer 1 associated with the enterprise 3. The alert serves to warn other users of possible problems.

[0023] In optional step 48, scan manager 32 checks to see whether a digital signature has been affixed to file 30, and, if so, verifies the digital signature with a trusted source in a conventional manner. If the digital signature is present and is verified by the trusted third party, scan manager 32 then rescinds the declaration of suspected malicious code found in step 44, and deems the file 30 to be clean after all.

[0024] The above description is included to illustrate the operation of the preferred embodiments and is not meant to limit the scope of the invention. The scope of the invention is to be limited only by the following claims. From the above discussion, many variations will be apparent to one skilled in the art that would yet be encompassed by the spirit and scope of the present invention.

[0025] The present invention can be implemented by a computer program operating on a proxy computer. An aspect of the present invention thus provides a storage medium storing processor implementable instructions for controlling a processor to carry out the method as hereinabove described.

[0026] Further, the computer program can be obtained in electronic form for example by downloading the code over a network such as the internet. Thus in accordance with another aspect of the present invention there is provided an electrical signal carrying processor implementable instructions for controlling a processor to carry out the method as hereinbefore described.

Claims

1. A method for detecting the presence of malicious computer code in an e-mail sent from a client computer to an e-mail server, said method comprising the steps of:

   allowing an e-mail proxy that is interposed between the client computer and the e-mail server to intercept e-mails sent from the client computer to the e-mail server;
   enabling the proxy to determine when a file is attempting to send itself as part of an e-mail; and
   declaring a suspicion of malicious code when the proxy determines that a file is attempting to send itself as part of an e-mail.

2. The method of claim 1 wherein the proxy resides within the client computer.

3. The method of claim 1 wherein the e-mail server and the proxy adhere to the SMTP protocol.

4. The method of claim 1 further comprising, in response to the declaring step, the step of sending a message to a user of the client computer.

5. The method of claim 4 wherein the message gives the user a plurality of choices, comprising at least one choice from the following group of choices:

   preventing the file from e-mailing itself;
   quarantining the file;
   allowing the file to send e-mail attachments; and
   always allowing the file to send e-mail attachments.

6. The method of claim 5 further comprising, when the user chooses to quarantine the file, the step of encrypting the file and sending the file to an antivirus software company.

7. The method of claim 1 further comprising, in response to the declaring step, the step of transmitting an alert to each computer in an enterprise associated with the client computer.

8. The method of claim 1 further comprising, in response to the declaring step, the step of rescinding the declaration of suspicion when the file contains a digital signature and the digital signature is verified.

9. The method of claim 1 wherein the enabling step comprises the substeps of:

decomposing the e-mail into constituent parts; and
determining that the file is attempting to send itself when a replica of the file is detected in one of the constituent parts.

10. The method of claim 1 wherein the enabling step comprises the proxy comparing a version of the file from the client computer with a version of the file from within the proxy.

11. The method of claim 10 wherein a suspicion that malicious code is present in the file is declared when the two versions are nearly identical.

12. The method of claim 11 when near identicalness is defined to mean that no more than one byte out of a preselected threshold number of bytes varies between the two versions.

13. The method of claim 12 wherein the preselected threshold number is 512.

14. Apparatus for detecting the presence of malicious computer code in an e-mail sent from a client computer to an e-mail server, said apparatus comprising:

a proxy computer interposed between the client computer and the e-mail server, said proxy computer comprising:

a redirector module adapted to intercept e-mails sent from the client computer to the e-mail server; and
coupled to the redirector module, a scan manager module adapted to determine when a file from the client computer is attempting to send itself as part of an e-mail.

15. The apparatus of claim 14 further comprising, coupled to the scan manager module, a decomposer module adapted to:

decompose e-mail into constituent parts; and
determine that the file is attempting to send itself as part of an e-mail when a near replica of the file is detected in one of the constituent parts.

16. A computer-readable medium containing computer program instructions for detecting the presence of malicious computer code in an e-mail sent from a client computer to an e-mail server computer, said computer program instructions performing the steps of:

allowing a proxy that is interposed between the client computer and the e-mail server to intercept e-mails sent from the client computer to the e-mail server;
enabling the proxy to determine when a file is attempting to send itself as part of an e-mail; and
declaring a suspicion of malicious code when the proxy determines that a file is attempting to send itself as part of an e-mail.

17. The computer-readable medium of claim 16 further comprising computer program instructions for, in response to the declaring step, sending a message to a user of the client computer giving said user a plurality of choices, comprising at least one choice from the following group of choices:

preventing the file from e-mailing itself;
quarantining the file;
allowing the file to send e-mail attachments; and
always allowing the file to send e-mail attachments.

18. The computer-readable medium of claim 17 further comprising computer program instructions for, when the user chooses to quarantine the file, encrypting the file and sending the file to an antivirus software company.

19. The computer-readable medium of claim 16 further comprising computer program instructions for, in response to the declaring step, transmitting an alert to each computer in an enterprise associated with the client computer.

20. The computer-readable medium of claim 16 further comprising computer program instructions for, in response to the declaring step, rescinding the declaration of suspicion when the file contains a digital signature and the digital signature is verified.

21. The computer-readable medium of claim 16 wherein the file is attempting to send itself as part of an e-mail body.

22. The computer-readable medium of claim 16 wherein the file is attempting to send itself as part of an e-mail attachment.

23. An electrical signal carrying processor implementable instructions for controlling a processor of a proxy computer to carry out the method of any one of claims 1 to 13.

FIG.1
PRIOR ART

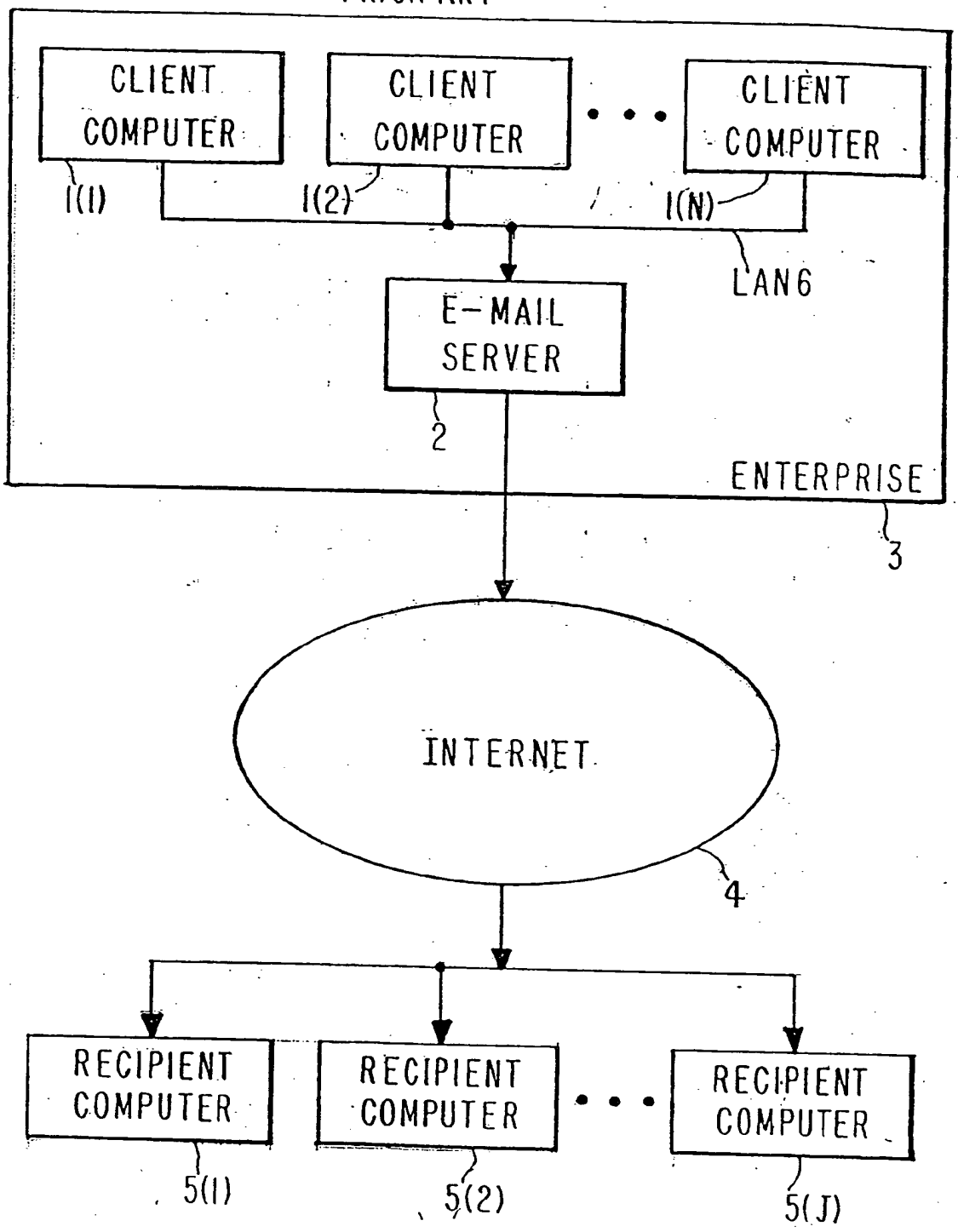


FIG.2
PRIOR ART

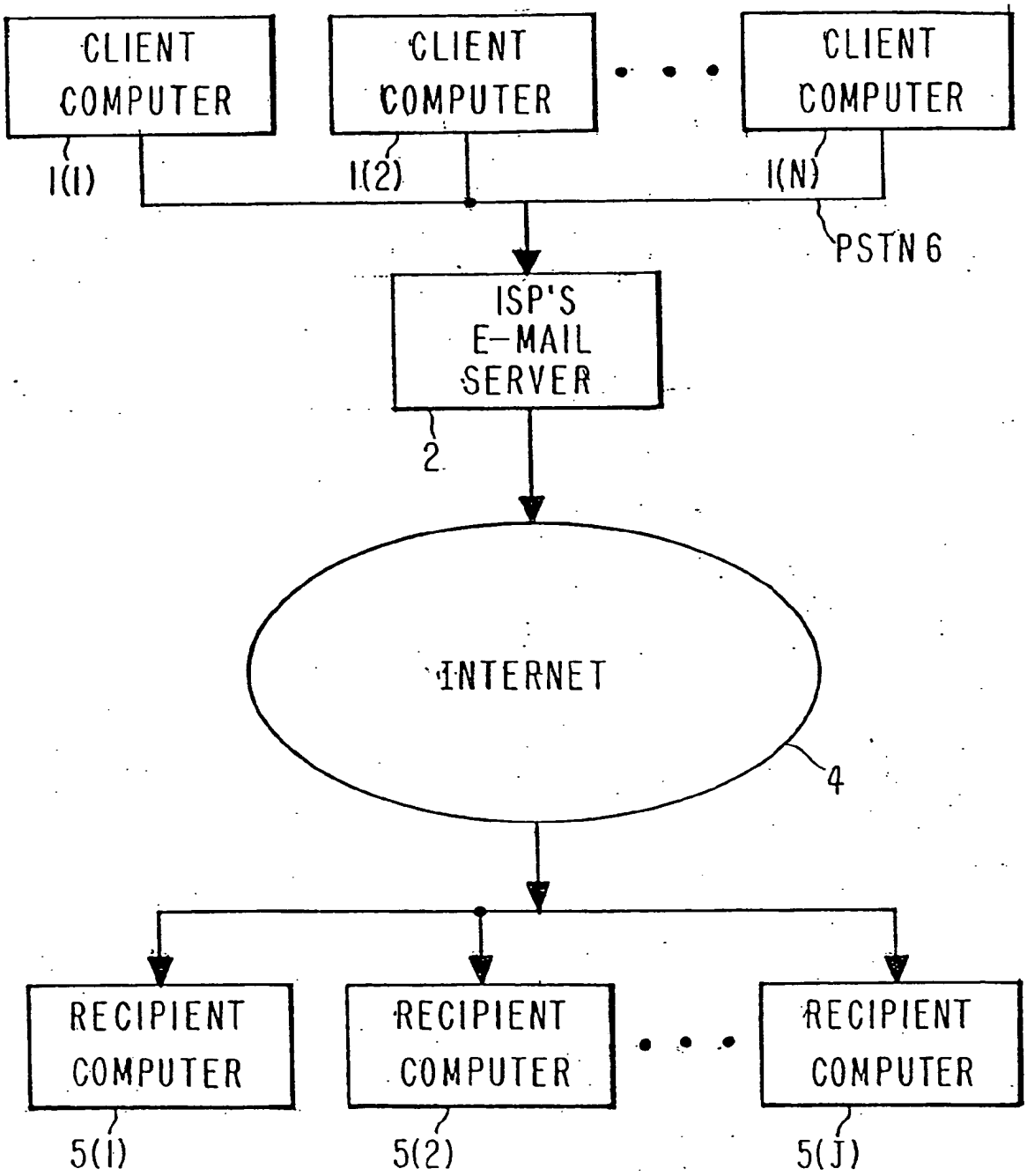


FIG. 3

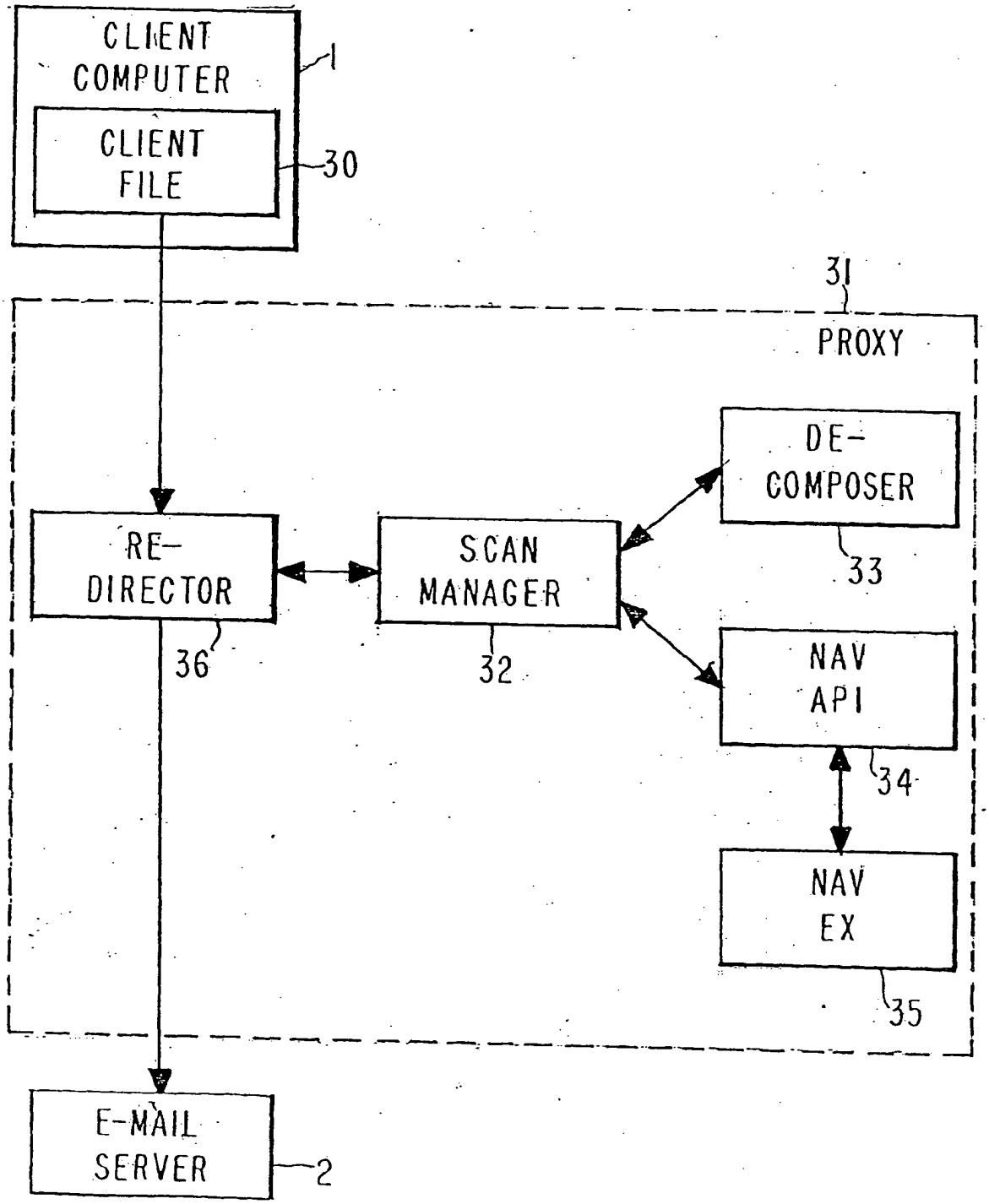


FIG. 4